

**North Carolina Security Breach Reporting Form**  
**Pursuant to the Identity Theft Protection Act of 2005**

\*Indicated a mandatory field

\*Name of the Company or Government Agency owning or licensing information affected by the entity experiencing breach:

NAPOLI SHKOLNIK PLLC

Entity Type: GENERAL BUSINESS

Address:

Apt/Suite/Building:

City:

State:

Zip Code:

Telephone:

Fax:

Email:

\*Date Security breach Reporting Form Submitted: 08/30/2018

Is this notice a supplement to a previously filed  
Security Breach: NO

\*Date the Security Breach was discovered: 07/09/2018

Breach Type: PHISHING

\*Estimated number of affected individuals: 1327

\*Estimated number of NC residents affected: 66

Name of company or government agency maintaining or possessing information that was the subject of the Security Breach, if the agency that experienced the Security Breach is not the same entity as the agency reporting the Security Breach (pursuant to N.C.G.S. 75-65(b))  
GARRETSON RESOLUTION GROUP, INC.

Describe the PLEASE SEE APPENDIX.  
circumstances  
surrounding the  
Security Breach:

Information Type: SSN

\*Regarding YES  
information  
breached, if  
electronic, was the  
information  
protected in some  
manner:

If YES, please GARRETSON RESOLUTION GROUP, INC. ("GRG") HAD SECURITY  
describe the MEASURES IN PLACE, INCLUDING ANTIVIRUS SOFTWARE, FIREWALL,  
security measures PASSWORD PROTECTION, LOGGING, AND OTHER SAFEGUARDS.

protecting the information:

\*Describe any measures taken to prevent a similar Security Breach from occurring in the future:

\*Date affected NC residents were/will be notified: 08/30/2018

Describe the circumstances surrounding the delay in notifying affected NC residents pursuant to N.C.G.S. 75-65 (a) and (c):

TO HELP PREVENT THIS TYPE OF INCIDENT FROM HAPPENING AGAIN, GRG IS TAKING ADDITIONAL STEPS TO ENHANCE ITS EXISTING NETWORK SECURITY MEASURES AND IS PROVIDING CONTINUED TRAINING TO EMPLOYEES ON THE DANGERS OF PHISHING E-MAILS.

GRG PROVIDED NOTICE TO THE INDIVIDUALS AS SOON AS POSSIBLE AND WITHOUT UNREASONABLE DELAY AFTER NAPOLI SHKOLNIK PLLC, GRG'S CLIENT, APPROVED ITS OFFER TO PROVIDE NOTIFICATION TO THE POTENTIALLY AFFECTED INDIVIDUALS.

**If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. 75-65(c), please attach or mail the written request or the contemporaneous memorandum.**

How NC residents were/will be notified? (pursuant to N.C.G.S. 75-65 (e)):

WRITTEN NOTICE

Please note if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2) , or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- Email notice when the business has an electronic mail address for the subject persons
- Conspicuous posting of the notice on the Web site page of the business, if one is maintained
- Notification to major statewide media

**Please attach a copy of the notice if in written form or a copy of any scripted notice if in telephonic form.**

Contact Information      ATTORNEY

Affiliation with entity  
experiencing breach:

Organization Name:      BAKER & HOSTETLER LLP

Prefix:      MR

\*First Name:      ERIC

Middle Name:

\*Last Name:      PACKEL

Suffix:

Title:      PARTNER

Address:      2929 ARCH STREET, CIRA CENTRE

Apt/Suite/building:      12TH FLOOR

City:      PHILADELPHIA

State:      PA      Zip Code:

19104

\*Telephone:      (215) 564-3031      Fax:

Email:      EPACKEL@BAKERLAW.COM

## North Carolina Security Breach Reporting Form - Appendix

Garretson Resolution Group, Inc. ("GRG") administers claims and settlement funds related to personal injury lawsuits and other matters. To perform these services, GRG's clients provide GRG with certain information regarding the settlement participants.

On August 8, 2018, after concluding its investigation of a security incident, GRG provided written notification to one of its clients about a security incident. The incident involved some personal information pertaining to settlement participants that the client had provided to GRG. As part of the written notification, GRG offered to provide notice to the affected settlement participants and to applicable regulatory agencies on the client's behalf. Pursuant to the client's direction, GRG is now providing notice of the incident to affected settlement participants and applicable regulatory agencies.

Through its investigation, which was conducted with the assistance of a leading cyber security firm, GRG determined that between April 4, 2018 and May 4, 2018, as a result of a phishing email, there was unauthorized access to four employee email accounts. GRG then undertook a comprehensive review of the emails and attachments that may have been accessed in the employees' email accounts and determined that one of the employees' email accounts contained certain personal information about settlement participants, including their names and Social Security numbers.

Additionally, the investigation confirmed that the incident did not involve unauthorized access to GRG's other networks or systems. GRG also purged the attackers from its email environment following the incident.

Beginning on August 30, 2018, GRG will mail notification letters to 66 North Carolina residents, in accordance with N.C. Gen. Stat. § 75-65, via United States Postal Service First-Class mail, in substantially the same form as the sample notice letter attached to this North Carolina Security Breach Reporting Form. GRG is offering all potentially affected individuals complimentary one-year memberships in credit monitoring and identity theft protection services from Experian®. GRG provided notice to the individuals as soon as possible and without unreasonable delay after GRG's client approved its offer to provide notification to the potentially affected individuals. To date, GRG is not aware of any misuse of the information.

To help prevent this type of incident from happening again, GRG is taking additional steps to enhance its existing network security measures and is providing continued training to employees on the dangers of phishing e-mails.



August 30, 2018

<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<City>><<State>><<Zip>>  
<<Country>>

Dear <<Name1>>:

The Garretson Resolution Group, Inc. (“GRG”) administers claims and settlement funds related to personal injury lawsuits and other matters. To enable us to perform these services, our clients provide us with certain information regarding the settlement participants. GRG places a high value on maintaining the integrity and security of this information. Regrettably, we are writing to inform you of an incident that involved some of your information, which was provided to GRG by your lawyers in connection with the lawsuit, *In Re: American Medical Systems, Inc.*, in which you are a participant. This notice describes the incident, the information involved, the measures we have taken, and some steps you can take in response.

On July 9, 2018, GRG concluded its investigation of a phishing e-mail incident. Upon first learning of the incident, we immediately took steps to secure the potentially affected employee e-mail accounts and began an internal investigation. We also engaged leading cyber security firms to assist with the investigation and further enhance the security of our systems. Our investigation determined that between April 4, 2018 and May 4, 2018, attackers gained access to certain employees’ e-mail accounts. As a result, some e-mails and attachments in the employees’ email accounts could have been accessed by the attackers, which contained your name, address, date of birth, and Social Security number. This incident did not involve unauthorized access to GRG’s other networks or systems and the attackers have been purged from GRG’s email environment.

Although, to date, we have no indication that any of your information was misused, out of an abundance of caution, we are informing you of this incident, and want to assure you that we take it very seriously. As a precaution, we have also arranged for you to receive a complimentary one-year membership of Experian’s® IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We deeply regret any inconvenience caused by this incident. To help prevent this type of incident from happening again, we are taking additional steps to enhance our existing network security measures, and we are providing continued training to employees on the dangers of phishing e-mails. If you have questions about this matter or the recommended next steps, please call 833-444-2698, Monday through Friday between 9:00 a.m. and 6:00 p.m., Eastern Time.



Sincerely,  
GARRETSON RESOLUTION GROUP

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **November 30, 2018** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-890-9332 to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-890-9332.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

### **ADDITIONAL STEPS YOU CAN TAKE**

Even if you choose not to take advantage of this complimentary credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**If you are a resident of Connecticut, Maryland, North Carolina, or West Virginia**, you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 888-743-0023 (toll free when calling within Maryland), 410-576-6300 (for calls originating outside Maryland)

*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 877-566-7226

*West Virginia Attorney General's Office*, State Capitol Complex, Bldg. 1, Room E-26, Charleston, WV 25305, [www.ago.wv.gov](http://www.ago.wv.gov), 800-368-8808

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)

**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)

**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or

password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.